blockchains

Review

Blockchain for Organ Transplantation: A Survey

Elif Calik [1] and Malika Bendechache [2,*]

[1] Department of Medical Engineering, Karabük University, Karabük 78050, Turkey; elifcalik@karabuk.edu.tr
[2] School of Computer Science, University of Galway, H91 TK33 Galway, Ireland
* Correspondence: malika.bendechache@universityofgalway.ie

Abstract: As blockchain becomes more widely used, a growing number of application fields are becoming interested in blockchain to benefit from its decentralised nature, invariability, security, transparency, quick transaction capabilities, and cost-effectiveness. Blockchain has a wide range of applications and uses in healthcare. Distributed ledger technology facilitates the secure transfer of patient medical records, manages the medicine supply chain, and creates an efficient, transparent, safe, and effective way of communicating data across global healthcare. The organ transplantation process (OTP) is one of the healthcare areas that benefit from the use of such technology to make its process more secure and transparent. In this article, we put forward a systematic literature review analysis on the application of blockchain to the OTP. Additionally, we address and highlight the barriers and challenges that arise while using blockchain technology for the OTP. We also offer some suggestions for future developments that would enhance blockchain's implementation in the OTP domain.

Keywords: blockchain; smart contract; distributed ledger; decentralised application; decentralised autonomous organisation; organ donation; organ transplantation

check for updates

Citation: Calik, E.; Bendechache, M. Blockchain for Organ Transplantation: A Survey. *Blockchains* **2024**, *2*, 150–172. https://doi.org/10.3390/blockchains2020008

Academic Editors: Keke Gai and Liehuang Zhu

Received: 16 February 2024
Revised: 25 April 2024
Accepted: 1 May 2024
Published: 9 May 2024

1. Introduction

The procedure of extracting an organ from a living or deceased donor and replacing it with an aligned recipient is referred to as the organ transplantation process (OTP), and it includes all the sub-steps that can be categorised as organ donation, allocation, matching, removal, transport, transplantation, and follow-up [1]. In this process, all transactions regarding the receiver and transmitter are recorded, stored, protected, and processed through conventional central database management systems. This data includes personal information and medical history. Therefore, this process consists of dynamic, fragile, and sensitive medical data. Moreover, this requires complex management of multi-stakeholder access to dynamic data. Along with the questions of how and where the data will be shared, by what method it will be stored, how its confidentiality and security will be ensured, and how the data ownership will be guaranteed and managed, the issues of how to ensure that the data is both anonymous, transparent, accountable, reliable, and traceable are becoming more important. Blockchain technology offers significant contributions to addressing data security challenges in sharing medical data. Its inherent features, which include a peer-to-peer (P2P) network [2,3], a decentralised structure, immutability, restricted read and write operations, and encrypted data, make it a promising solution. In the context of healthcare, where the protection of sensitive patient information is paramount, blockchain provides a robust and secure framework for data management. Overall, the combination of these features makes blockchain technology a promising solution to improve data security in the sharing of medical data, fostering trust, privacy, and integrity in healthcare systems. However, it is important to acknowledge that the adoption of blockchain in healthcare requires the careful consideration of legal, regulatory, and interoperability challenges to ensure its effective implementation and integration within existing healthcare infrastructures. From this point of view, blockchain can offer an effective solution to the challenges and issues [4,5] encountered in the OTP (see Figure 1).

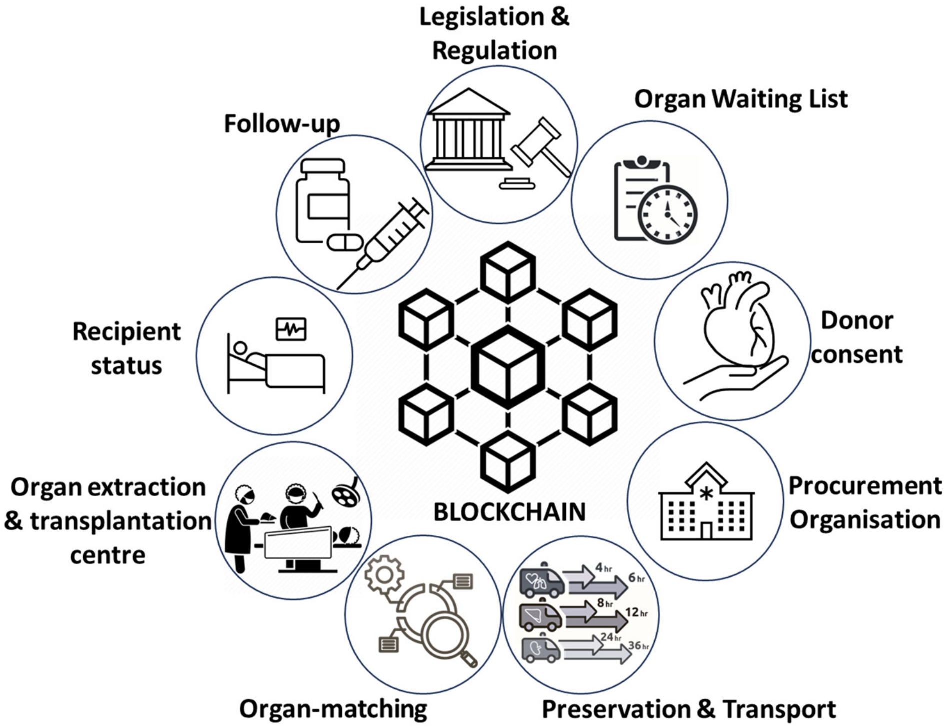

Figure 1. Organ transplantation process based on blockchain.

The nature of the OTP process inherently comprises intricate procedures and interwoven structures. Typically, this process is managed by the procurement organisation mandated by the authority within the framework of existing legislation and regulations. One of the significant challenges outlined in Figure 1 is the organ waiting list directly associated with the recipient. These lists are established and updated by applying different prioritisation protocols based on the type of organ, with the most crucial challenge being to ensure the fairness, reliability, accountability, and transparency of waiting lists. The second category of challenges revolves around the donor and associated issues, with organ donation consent being paramount among them. Given the variations in organ type, donor age, living or deceased status, and even the cause of death, it is imperative for this process to be conducted within the parameters of trustworthiness, fairness, security, and privacy. In the organ extraction centre, it is essential to ensure that appropriate conditions are maintained to prevent tissue death after the organ is removed from the donor. Additionally, there is a need to ensure that information regarding the transport of the organ to the recipient's transplantation centre, under suitable conditions, is secured. This process, known as preservation and transport, is carried out either concurrently or subsequently with the organ-matching process, both of which must be executed in a traceable, accountable, secure, fair, and privacy-preserving manner. Organs extracted from donors are transplanted to the recipient at the transplantation centre. The process, including a follow-up, varying in duration based on the type of transplanted organ, is documented. It is crucial that the data recorded during the follow-up process allows retrospective analysis in both the short and long terms. Additionally, attention should be paid to ensuring data integrity, data origin authenticity, and safeguarding against data manipulation [6–9].

While blockchain could offer an effective solution to the challenges in the OTP, concerns persist regarding the sensitivity of recipient and donor information in terms of the fundamental rights outlined in the General Data Protection Regulation (GDPR), such as the right to deletion, correction, and obtaining information about who can access their data. Despite research proposing solutions to this issue, debates continue. [10]. Another issue discussed is the potential challenges and solutions encountered in the development, testing, and deployment of smart contracts used in the automation of the system [11]. The success of smart contracts is directly proportional to the accuracy and reliability of the data sources they interact with. Smart contracts may lead to undesired outcomes when data accuracy and reliability are not ensured.

In the OTP, the efficient management of time-dependent scarce resources is crucial. Therefore, defining it as a system with zero error tolerance would be a very accurate approach.

From this standpoint, the OTP can be approached through a supply chain management (SCM) perspective. The important thing in this case is the irreplaceable nature of the product once it is lost. From an SCM perspective, we can outline the advantages of processing organ transplantation-related data on a blockchain as follows. The first category is transparency and traceability. Blockchain can record every step of the OTP, allowing all stakeholders to track transactions in real-time. This ensures full transparency in the supply chain and verifies every step, from the origin of organs to their delivery to recipients. The second category is data integrity and immutability. Blockchain technology serves as an immutable ledger, updated after each transaction and shared among all participants. This guarantees the integrity and immutability of OTP data, facilitating easy verification of data origin. The third category is automated transactions without third parties. Blockchain supports automated transactions through smart contracts, enabling predefined transaction steps in the OTP to occur automatically. Thus, it affects the increase in transaction speed and efficiency. Lastly, there is the verification and authorisation category. Blockchain enables all OTP stakeholders to verify and authorise their identities, resolving potential disputes between nodes through consensus mechanisms to maintain the reliability and integrity of the blockchain. This facilitates reliable and secure information sharing in the SCM process. To summarise, blockchain can support the resolution of supply chain challenges in the OTP, such as manipulation, origin, tracking, transparency, and accountability [12,13].

The adoption of disruptive technology is as crucial as the anticipated innovations it brings. It would not be wrong to say that the strength of blockchain can be measured by its adoption, which is one of its weakest links. A study conducted by [14], which examines blockchain adoption in the context of OTP, where traditional methods are currently employed, underscores the importance of this issue. Its findings suggest that blockchain can be effectively utilised to address the issues related to counterfeit drugs and medical equipment, thereby improving lives. However, findings also highlight societal concerns regarding blockchain, particularly regarding data privacy and security. Some of these concerns revolve around patients' desires to keep their health records confidential, who can access these records, and fears of potential misuse. Addressing these concerns will be essential to promote the adoption of blockchain technology in healthcare.

On the other hand, the challenge of the blockchain-based OTP system is primarily related to its difficulties in transforming the centralised approach to information management into a decentralised structure while maintaining the security and privacy of sensitive and personal data. Upon closer inspection, it became evident that the surveys and systematic reviews [15–18] that have been carried out up to this point have focused more on the conceptual frameworks than the technical components of the articles they have included. From a technical standpoint, it was found that they frequently considered the chain type and blockchain platform.

Ref. [15] has examined the six studies on blockchain-based organ transplantation in terms of the blockchain platform used and the contributions they provided. Accordingly, it was stated that in addition to the potential benefit of blockchain, there is a need to conduct research on data management systems that can work together with these systems. The five studies on blockchain-based organ transplantation evaluated by the survey in [16] were examined in terms of the blockchain platform used and the contributions they made, similar to [15]. According to their reviews, in order to create smart contracts, they are of the opinion that the common factors, policies, and guidelines between peers in the network should be well defined in advance. Moreover, in this context, the need for international regulations is also underlined. Another survey [17] has examined eight studies on blockchain-based organ transplantation. The examined studies were evaluated in terms of the platform used, chain type, and contribution, as in [15,16]. Unlike previous surveys, it lacks structured assessment content. The survey highlights the lack of trust in digital systems and the immaturity of blockchain technology as challenges. It is reported that in order to identify full nodes in private blockchain networks—which have an entire copy of the blockchain and validate every block and transaction—detailed research is needed. In the comprehensive literature review conducted by [18], organ transplantation applications were investigated as one of the primary domains among six. It is noteworthy to mention that only Kidner [19] was incorporated into this review. The articles considered in the review were assessed with respect to a blockchain platform, chain type, and consensus. The study highlights the role of blockchain in streamlining and expediting the donation processes. Additionally, it is pointed out that the scalability of data stored in such systems is currently a topic of debate. Furthermore, the transition from the existing system to a blockchain-based system is anticipated to pose challenges in terms of cultural, trust-related, and regulatory aspects.

The study carried out in [20] regarding the integration of blockchain technology in healthcare underscores the need for a careful adaptation to the healthcare sector, suggesting that blockchain should not be implemented in its current state. It also suggests that employing blockchain for monitoring donated organs throughout the entire transplantation process holds the potential to enhance operational efficiency. Moreover, the incorporation of blockchain with existing technologies introduces a layer of innovation to the overall process. Moreover, the utilisation of smart contracts allows for process automation, as highlighted in the study. According to [21], attention was drawn to the blockchain-based decentralised systems developed for organ transplantation, which is one of the fields of study of surgical sciences. It was emphasised that surgical sciences should also take an active role in the development of such systems with the potential of a solution. In [22], emphasis was placed on the necessity for policymakers to formulate comprehensive privacy policies aiming to cultivate trust in emerging technologies, particularly in the context of blockchain-based organ transplantation systems. In [23], an analysis was conducted on all participants within the organ transplantation supply chain and their respective roles throughout the life cycle. The study highlights that inadequate access to data in the organ supply chain managed through centralised approaches or doubts regarding the accuracy of the data can lead to biased or unreliable decisions within this process (such as organ compatibility and donor-recipient matching). Thus, the selection of chain types and methods for data storage, particularly off-chain, is of significant importance. Furthermore, there is an emphasised necessity to establish a legal framework. Utilising the qualitative content analysis approach outlined in [24], the study delved into the impact of AI and blockchain on organ/tissue transplantation. The authors underscored the necessity for a consolidated digital interface and the integration of emergency health services to streamline operational procedures during organ transplants. Moreover, they also emphasised the importance of standardising organ transplantation processes. Investigating the adoption of blockchain technology, [25] assessed both the domestic and global instances of blockchain-based applications. The evaluation encompassed factors influencing adoption, potential opportunities, and challenges within these applications. The study introduced the “Hayat donor registry” as one of the six use cases within the national corporate blockchain. This specific application was designed to ensure the secure and transparent management of organ donation processes. In this manner, the need for good corporate practice examples for blockchain adoption was emphasised. As in [18], Kidner [19] was cited in [26] as an example of how blockchain was being used in the healthcare industry. It was additionally highlighted that blockchain technology is still in its early stages of maturation, which was also addressed.

When analysing the reviews and surveys concerning the OTP, it becomes evident that they explored the conceptual aspect of the subject, its adoption, the field-specific roles it assumes, and its fundamental contributions to science. Additionally, it has been observed that the OTP is regarded as a subsection within the broader context of blockchain applications in healthcare. However, we found that the technical aspect often does not go beyond considerations of the platform used, chain type, and consensus level.

To the best of our knowledge, no comprehensive review paper has explored blockchain and its applications for the OTP from both theoretical and technical viewpoints. This paper aims to address this gap by carrying out a systematic literature review, encompassing all relevant studies examining the use of blockchain for the OTP. We analyse and discuss these works, shedding light on the challenges and limitations related to using blockchain technology for OTPs. Additionally, we suggest potential avenues for future research and development to enhance the effectiveness of blockchain in OTP applications.

The key contributions of this article that distinguish it from others are summarised as follows:

- We provide a comprehensive literature review that concentrates on not only the theoretical but also detailed technical scopes of blockchain applications in the OTP.
- To provide new research opportunities for scholars in this field, we outline the technical maturity levels of the solutions proposed in the reviewed publications and propose potential directions for future research.

The remainder of this paper is organised as follows: Section 2 provides a brief overview of the main technologies used in this survey study. Section 3 details the methodology used in our systematic review, whereas Section 4 reports and analyses the works selected from our systematic review methodology. Section 5 summarises the list of issues and challenges found. Finally, Section 6 concludes the paper.

2. Background

Blockchain technology, which has gained significant recognition in the field of cryptocurrency, was introduced to the scientific community through the publication of a whitepaper by Satoshi Nakamoto in 2008 [27–29]. However, it is important to acknowledge other technical advancements that have contributed to the development of blockchain technology [30]. Among the notable ones, we can mention the "Merkle Tree", developed by Ralph Merkle in 1979, which serves as a digital signature method and helps maintain the integrity of transactions on the blockchain [31,32]. Additionally, in 1982, David Chaum proposed "a new cryptographic method" that could enable automatic payment systems where third parties cannot access information, provide payment proofs and the identity of creditors, and prevent double-spending of payment instruments in cases of theft [33]. Another significant development was the "timestamp" introduced by Stuart Haber and W. Scott Stornetta in 1991, aiming to prevent users from backdating or forward-dating digital records [34,35]. In 1996, Szabo created "Smart Contracts" to facilitate direct interaction between two parties on the blockchain without the need for intermediaries [29]. In 1997, Adam Back presented "Hashcash" as a method to reduce spam, which is now utilised as the "proof-of-work" for adding new blocks to the blockchain [36,37]. Nick Szabo's contribution in 1998 with "Bit Gold" was described as a reliable electronic monetary system that could operate without a central authority, enabling secure and transparent transactions and serving as a precursor to Bitcoin [38]. Wei Dai's "B-money", also from 1998, proposed a decentralised, secure, anonymous digital currency for peer-to-peer transfers [39]. Peer-to-peer (P2P) networks gained popularity with Napster, which was developed by Shawn Fanning in 1999 for file sharing, especially used for sharing music files [40]. Hal Finney's "Reusable Proof of Work (RPOW)" in 2004 addressed the double-spending problem [41]. Lastly, Satoshi Nakamoto's groundbreaking application of Bitcoin in 2008 brought together the pieces of the puzzle, culminating in the historical development of blockchain technology [27]. Alongside these developments, it is essential to include the terms distributed ledger, a decentralised application (Dapp), and decentralised autonomous organisation (DAO), which we have identified as closely intertwined concepts with blockchain, to framework our study. A distributed ledger is a database where all transactions executed in a network with multiple participants are recorded, and identical copies of this ledger are distributed to all participants in the network. Any changes are immediately reflected in the ledger. All copies held by the participants are updated almost instantly. The security and accuracy of the data in the distributed ledger are protected by cryptographic keys and signatures. In this way, trust is established between parties who do not trust each other. Furthermore, it is important to note that while all blockchains are distributed ledgers, not all distributed ledgers are blockchains [42].

Dapp is an application that operates on a decentralised network rather than a centralised server. It utilises blockchain technology or other decentralised technologies to facilitate peer-to-peer interactions and eliminate the need for intermediaries [43,44].

A decentralized autonomous organization (DAO) is an organisation that operates through rules encoded as smart contracts on a blockchain. These smart contracts define the governance rules and decision-making processes of the organisation, allowing it to function autonomously without the need for centralised control or intermediaries. This model disperses power and decision-making processes, fostering a structure for the organisation that is more transparent, equitable, and participatory [45].

2.1. Technological Evolution of Blockchain

The technological evolution of blockchain has been approached through various categorisations in different sources, exhibiting differences in the grouping. By adopting a generational approach, it is possible to address the stages of blockchain's technological evolution in the following categories [4].

The first phase, referred to as Blockchain 1.0 or the "Transaction" generation, encompasses the development of digital currency. The best-known application example is Bitcoin. Its key characteristics include distributed digital currency creation, consensus mechanisms, and a secure, transparent, and immutable ledger known as a distributed ledger [27,46].

The second generation, Blockchain 2.0 or the "Smart Contract" generation, focuses on the development of programmable blockchain and smart contracts. Smart contracts enable the encoding of predefined agreements between parties into electronically executable code, operating under specific conditions. They also operate autonomously, securely, and transparently without the need for intermediaries. The Ethereum platform is the most prominent example of facilitating the use of smart contracts. The fundamental characteristic of this generation is the extension of blockchain technology to use cases beyond currency [44,46].

The third generation, Blockchain 3.0 or the "Application" generation, encompasses the development of distributed and secure Dapp in various domains, ranging from healthcare to industries. Dapp operates on blockchain-based platforms, utilising smart contracts containing code snippets that execute automatically under specific conditions. Decentralised applications can be developed for various use scenarios, such as supply chain management, social media, and decentralised finance (DeFi). Ethereum, EOS, and TRON are well-known systems in this domain [4,44,46].

The current and emerging generation is Blockchain 4.0, or the "Digital Society" generation, which is characterised by advanced features, sustainability, and integration with other technologies. Current advancements in this phase include the decentralised web and Relictum pro, as well as industrial applications like R chain and metaverse—which we might loosely classify as the Internet of Everything (IoE). It is anticipated that this phase will encompass advancements and more in areas like advanced features, sustainability, and integration with other technologies [4].

2.2. Structure of Blockchain

Blockchain operates on a chain structure where validated transactions are systematically added in the form of blocks as irreversible inputs. Hence, once a transaction concludes, it becomes unalterable, indestructible, and irremovable. This unique characteristic elevates blockchain systems above centralised solutions. They are briefly defined as decentralised distributed ledgers, blockchain functions by sequentially transforming transactions into blocks using timestamps and cryptographic hashes. These blocks are then interconnected based on the order of transactions. The Merkle root hash stores the hash of each block's transaction records. The timestamp includes the current time in seconds. Each new block, while appended to the end of the preceding one, carries the hash of the previous block. The initial block in the chain, commonly known as the Genesis block, has a hash value of zero. The cryptographic one-way hash function SHA256 is utilised to create the hash value connecting the blocks. Consequently, the block inherits the qualities of anonymity, immutability, and compactness. Peers in the blockchain—also referred to as nodes—are interconnected through peer-to-peer (P2P) networks. Digital signatures stand out as a primary technique for ensuring the security and accuracy of the data stored on the blockchain. Each peer within the network possesses a public and private key pair for this purpose.

The fundamental structure of a blockchain can be described as the storage of electronically executed transactions between parties in a shared ledger distributed over a network. Its general architecture, as depicted in Figure 2, consists of application, contract, consensus, network, and data layers [27,47,48]. In general, the OTP solutions based on blockchain are developed within the application layer and contract layer.

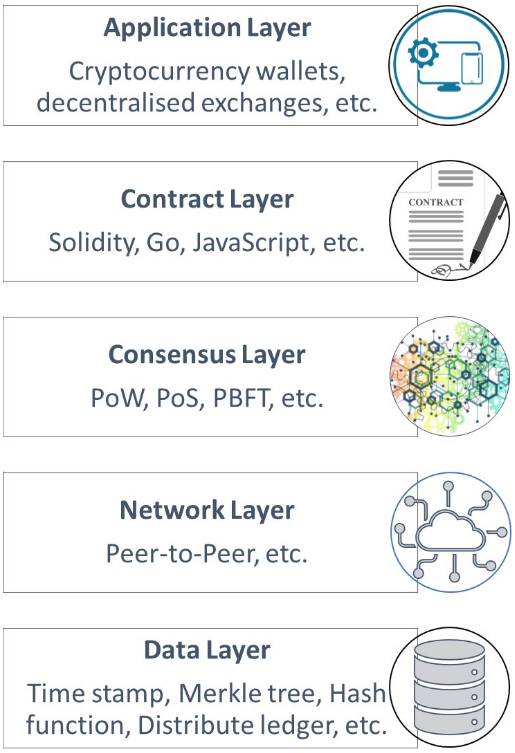
Application Layer
Cryptocurrency wallets, decentralised exchanges, etc.
Contract Layer
Solidity, Go, JavaScript, etc.
CONTRACT
Consensus Layer
PoW, PoS, PBFT, etc.
Network Layer
Peer-to-Peer, etc.
Data Layer
Time stamp, Merkle tree, Hash function, Distribute ledger, etc.

Figure 2. Basic blockchain architecture.

The workflow of a typical blockchain encompasses various steps. There are the crucial steps in the blockchain workflow, as seen in Figure 3 below: (i) The process begins with the creation of a transaction, where a participant initiates a transfer of assets or data on the blockchain network (for instance, incorporating the organ extracted from either a living or deceased donor into the list for organ distribution); (ii) the transaction is then broadcasted to the network, ensuring that all participating nodes are aware of the transaction (for instance, donor, recipient, healthcare professionals, etc., on the network are informed about this); (iii) the nodes in the network check the validity and authenticity of the transaction, including verifying syntax, digital signatures, authorization, and preventing double-spending (for example, the procurement organisation verifying data on the network in accordance with existing legislation and regulations); (iv) verified transactions are grouped together into a block, forming a chronological sequence of transactions (for instance, such as the order of each organ extracted from the donors is being added to the network); (v) the network participants reach a consensus on the validity of the block, typically through a consensus algorithm that ensures agreement among the majority of nodes (for instance, such as the order of each organ extracted from the donors is being added to the network); (vi) once consensus is achieved, the validated block is added to the blockchain, becoming part of the permanent and immutable record (such as ensuring the immutability of the organ data to be transplanted); (vii) the ledger, which represents the current state of the blockchain, is updated to reflect the new transactions added to the blockchain (such as creating an immutable record of organs to be transplanted) [47].

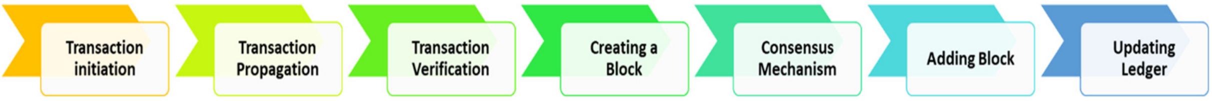

Figure 3. Blockchain workflow diagram.

The following section describes our review methodology used to gather the relevant papers included in our literature review analysis.

3. Methodology

The systematic review phases outlined in this research paper have been executed in accordance with the widely recognised guidelines and stages outlined in [49–52]. In computer science, the fundamental components of a systematic review typically include: (i) formulating research inquiries, (ii) determining the search strategy, (iii) identifying inclusion and exclusion criteria for selected studies, (iv) extracting relevant data from the selected studies, (v) analysing and synthesising the acquired data, and (vi) presenting the findings of the systematic review in a clear and structured manner.

3.1. Research Inquiries

To conduct this survey, the following research questions were determined:

- Q1: Has any research been conducted that examines the blockchain-based technologies in the OTP?
- Q2: What are the typical blockchain technology applications used for the OTP?
- Q3: Which blockchain platforms and types are the most used in the OTP?
- Q4: Which environments are primarily used for validating the suggested systems?
- Q5: What are the challenges (if any) that are hindering the implementation of blockchain technology for the OTP?

3.2. Determination of the Search Strategy

Following the creation of the research questions, the review methodology was established to delineate the search strategies and inclusion/exclusion criteria for the studies. The review methodology is outlined as follows:

Initially, a set of keywords was devised for use in constructing our search query. To ascertain the most pertinent keywords, two researchers independently conducted preliminary searches. Subsequently, a consensus was reached on the final list of keywords to be utilised.

Subsequent to the keyword selection, these terms were combined into a structured search query employing Boolean operators, enabling searches across various digital libraries. The digital repositories utilised included (i) SpringerLink, (ii) ScienceDirect, (iii) IEEE Xplore, (iv) ACM Digital Library, (v) Scopus, (vi) Web of Science, (vii) Medline (via PubMed), and (viii) Embase.

To ensure objectivity and consistency in managing the articles included in the study, we employed the reference management software JabRef 5.12 [53]. A Microsoft Excel spreadsheet was utilised to collate the retrieved papers.

The details of the search query and the digital libraries employed are summarised in Table 1.

Table 1. The search string and query results.

The Search String	Databases	Query Results
("blockchain" OR "smart contract?" OR "distributed ledger" OR "decentralized application" OR "decentralized autonomous organization") AND ("organ" OR "liver" OR "kidney" OR "pancreas" OR "lung" OR "heart") AND ("donation" OR "transplantation")	SpringerLink	419
	ScienceDirect	302
	IEEE Xplore	13
	ACM Digital Library	83
	Scopus	29
	Web of Science	9
	MEDLINE (via PubMed)	5
	Embase	5
TOTAL		865

The initial search query yielded a total of 865 research papers relevant to the topic under investigation. To ensure a systematic and replicable selection process, a set of inclusion and exclusion criteria, as outlined in Table 2, was established. Upon review, 150 papers were identified as duplicates and consequently removed, reducing the total number of papers to 715.

Table 2. The inclusion and exclusion criteria.

The Inclusion Criteria	The Exclusion Criteria
- Full text - Published at any time - Published in the English language - Published in the chosen digital libraries - Published in workshops, symposiums, conferences, journals, and book chapters - A study manuscript on blockchain technology for the organ transplant process	- Incomplete studies - Published as a letter, review - Duplicated studies - All studies that did not meet the inclusion criteria - A study manuscript on blockchain technology for blood and charity donation

Following the methodology proposed by Kitchenham et al. [45–48], two researchers independently screened the titles of the remaining papers. This title-based screening process resulted in the exclusion of a significant portion of papers, leaving 56 papers for further consideration. Subsequently, the abstracts of these papers were carefully examined, leading to the exclusion of additional papers and reducing the number to 31.

In the subsequent phase, the full texts of the remaining papers were thoroughly reviewed. Throughout all three phases of screening, any disagreements regarding the inclusion or exclusion of a paper were resolved through discussions until a consensus was reached.

Following the meticulous application of these selection criteria, 22 pertinent papers were ultimately identified for inclusion in the study.

To make sure all relevant papers are returned, a "snowballing" approach was also used to add more relevant papers. To achieve this, we first went over each reference in the 22 papers returned by our search string that satisfied the inclusion requirements indicated in Table 2. Following that, we also examined articles that referenced these 22 articles. Using this approach, we were able to include 13 additional articles. Thus, 35 relevant papers were included in our final review study. These papers are summarised in Section 4.1.

3.3. Extracting Data

The data collected from each of the articles included in the survey encompassed bibliographic details, the objective of the blockchain application, the utilised platform, the category of the chain, the implementation method of the solution, whether testing and verification procedures were conducted, analytical metrics employed, and the type of platform utilised. The distribution of publications by year is illustrated in Figure 4. After a thorough examination of the full-text articles, quantitative analysis was performed on 35 papers.

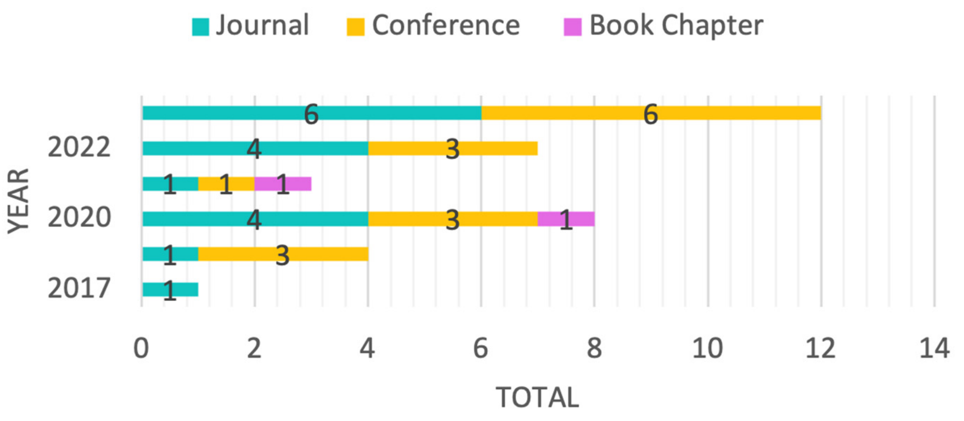

Figure 4. Number of publication types per year.

4. Review Results

The publications that we gathered from our systematic review are examined in this section. First, we look over their bibliographic information, including the number of publications they make annually, the kinds of publications they produce, and the publishers. Then, we take an in-depth look at their content, proposed techniques, testing techniques, and types of metrics.

4.1. Preliminary Results

As seen in Figure 4, the application of blockchain technology to the organ transplantation process is a relatively novel area, with the first study published in 2017 (Data were collected until 31 December 2023). An increasing number of studies on this unique topic, totaling 35, reflects the growing importance and sensitivity of the subject.

Regarding the publication types, approximately half of the publications (17 out of 35) were journal articles, 16 were conference papers, and two were book chapters (Figure 4).

As can be seen in Table 3, the dominant publication platform was IEEE Access (17 out of 35 publications). Next, Springer followed with two publications. Wiley and ScienceDirect then followed with a publication each.

Table 3. Distribution of selected publications by preliminary categories.

No.	Author(s)/Ref.	Year	Topic	Publication Type
1	Zouarhi [19]	2017	Kidner—A Worldwide Decentralised Matching System for Kidney Transplants	Journal
2	Alandjan [54]	2019	Blockchain Based Auditable Medical Transaction Scheme for Organ Transplant Services	Journal
3	Dajim et al. [55]	2019	Organ Donation Decentralized Application Using Blockchain Technology	Conference
4	Lamba et al. [56]	2019	Preventing Waiting List Manipulation and Black Marketing of Donated Organs Through Hyperledger Fabric	Conference
5	Ranjan et al. [57]	2019	Decentralised and Distributed System for Organ/Tissue Donation and Transplantation	Conference
6	Morande and Marzullo [24]	2020	Application of Artificial Intelligence and Blockchain in Healthcare Management-Donor Organ Transplant System	Journal
7	Chavez et al. [23]	2020	Securing Transparency and Governance of Organ Supply Chain Through Blockchain	Book Chapter
8	Daniel et al. [58]	2020	A Blockchain based solution for Managing Transplant Waiting Lists and Medical Records	Conference
9	Gaynor et al. [20]	2020	Adoption of Blockchain in Health Care	Journal
10	Kulshrestha et al. [59]	2020	Securing Organ Donation using Blockchain	Journal

Table 3. *Cont.*

No.	Author(s)/Ref.	Year	Topic	Publication Type
11	Niyigena et al. [16]	2020	Survey on Organ Allocation Algorithms and Blockchain-based Systems for Organ Donation and Transplantation	Conference
12	Pillai et al. [60]	2020	An Effective Protection of Data for Organ Donation Using Blockchain Technology	Journal
13	Wijayathilaka et al. [61]	2020	Secured, Intelligent Blood and Organ Donation Management System—"LifeShare"	Conference
14	Yahaya et al. [62]	2021	An Organ Donation Management System (ODMS) Based on Blockchain Technology for Tracking and Security Purposes	Conference
15	Alam and Raza [26]	2021	Chapter 7—Blockchain Technology in Healthcare: Making Digital Healthcare Reliable, More Accurate, and Revolutionary	Book Chapter
16	Soni and Kumar [63]	2021	Creating Organ Donation System with Blockchain Technology	Journal
17	Begum et al. [64]	2022	OraB—A Community of Donors	Conference
18	Çalık et al. [65]	2022	A Novel Method to Ensure the Security of the Shared Medical Data Using Smart Contracts: Organ Transplantation Sample	Journal
19	Chaudhary et al. [66]	2022	Organ Bank Based on Blockchain	Conference
20	Hawashin et al. [67]	2022	Blockchain-Based Management for Organ Donation and Transplantation	Journal
21	Yashwanth Kumar and Supreetha [68]	2022	Smart NGO Tracking System Using Blockchain Technology	Conference
22	Sarier [69]	2022	Privacy Preserving Biometric Authentication on the Blockchain for Smart Healthcare	Journal
23	Carrano et al. [21]	2022	Blockchain in surgery: are we ready for the digital revolution?	Journal
24	Ajay et al. [70]	2023	A Web DApp for Efficient Organ Donation Management System: Leveraging Centralized Wallet Architecture as Backend	Conference
25	Anselmo et al. [15]	2023	Implementation of Blockchain Technology Could Increase Equity and Transparency in Organ Transplantation: A Narrative Review of an Emergent Tool	Journal
26	Divyashree and Ravi [71]	2023	Blockchain-Based Access-Control System for Unused Medicine and Organ Donation Using Enhanced Hybrid Cryptography	Conference
27	Ghosh and Dutta [72]	2023	Indriya: Building a Secure and Transparent Organ Donation System with Hyperledger Fabric	Journal
28	Shyamala Gowri et al. [73]	2023	Organ Donation and Transplantation Framework based on Ethereum Blockchain	Conference
29	Hovorushchenko et al. [74]	2023	Blockchain-Based Medical Decision Support System	Journal
30	Kayalvili et al. [75]	2023	Management of Organ Donation Using Dapp in Blockchain	Journal
31	George and Kizhakkethottam [17]	2023	A Survey on the Impact of Blockchain in Effective Organ Transplantation	Conference
32	Thaker et al. [76]	2023	ORGANiser	Conference
33	Varshney et al. [22]	2023	Policy Suggestions for Transplantation of Organs in India: Use of Blockchain Technology to Manage Organ Donation	Journal
34	Soltanisehat et al. [18]	2023	Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review	Journal
35	Shuhaiber et al. [25]	2023	Breaking Boundaries: Exploring Blockchain's Impact on UAE Organizations	Conference

4.2. Blockchain Technologies Used for OTP

This section examines the blockchain technologies utilised for OTP, paying close attention to the maturity of their solution. From the 35 relevant returned papers, we identified 24 papers that are actual technical solutions for the application of blockchain to the OTP. We have categorised these papers based on the maturity of their solution as follows: (i) conceptual solution, (ii) in-house validated solution, and (iii) fully validated solution.

When we analysed the solutions offered by the articles based on their maturity levels, we determined that more than half of them (17 out of 24) were solutions that were validated in-house using an in-house test bed. Thus, no real deployment was conducted for these solutions. Seven articles were at the conceptual level, where the proposed solutions are just theoretical with no real testing or validation. None of the reviewed papers offered a fully validated solution with a real deployment (Figure 5). This clearly shows that there are more validated solutions that keep emerging in recent years compared to the conceptual ones. However, it is also clear that there is a lack of more mature blockchain solutions in this domain (Figure 5).

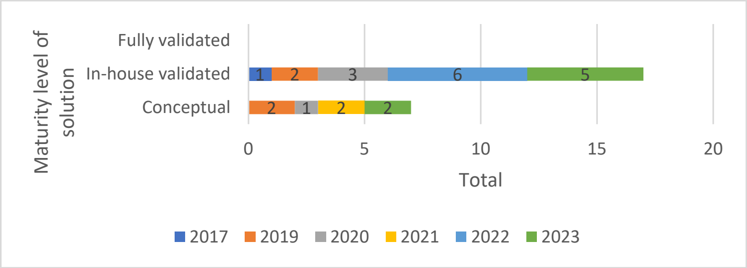

Figure 5. Level of maturity of solutions offered by the reviewed papers.

4.2.1. Conceptual Blockchain Solution

In this section, we explore seven papers that put forth the idea of developing blockchain frameworks for the OTP. These papers introduce their overarching proposed architectures and touch upon certain aspects and characteristics of their proposed designs at a broad level. For instance, ref. [62] addresses the inclusion of on-chain provisioning and data integrity logic for medical data sources. This enables individuals to ensure record originality, auditability, and control over data sharing. However, it is observed that the reported solution has not yet advanced to the implementation stage. In another study [73], it is reported that the development, testing, and verification of "smart contracts" were conducted using the private Ethereum platform. However, no implementation, verification, or test result sharing was offered, even though theoretical details regarding the general design and modules of the suggested system were shared.

Ref. [60] suggests a way to protect donor data on the blockchain by using public key cryptography for identity verification, which guarantees safe device and person identification. However, there is no evidence in their articles demonstrating any experimentation conducted on the blockchain. In [54,55,63,74], the authors focused on providing the general features of blockchain, its working principle and related work, and the application framework of the proposed systems were presented. However, the lack of details regarding the blockchain's platform, chain type, smart contracts, storage features, and validation indicators for the proposed system in these publications indicates that the solutions presented in these articles are conceptual or at the early stage of their development. Thus, they lack maturity.

4.2.2. In-House Validated Blockchain Solution

In this section, we discuss the remaining 17 papers with higher levels of maturity solutions, which not only proposed the use of blockchain for the OTP but also provided an in-house validation of their solutions. We compared these papers based on the test and validation metrics used, as well as the environments selected or created for testing and validation. By doing this, we clarified the approaches used to determine if the suggested solutions in these articles satisfy the expected performance criteria and conform to the standards. The solutions provided by the paper encompass a broad spectrum of applications, including simulations of the stages of a transaction conducted between parties on the web, along with the utilisation of specialised test environments for measuring throughput, latency, successful/failed transaction counts, and gas consumption.

The provision of security is typically identified as the primary goal when the studies are analysed according to their objectives. This is followed by ensuring transparency, tracking, reliability, confidentiality, and trustworthiness. Among the biggest concerns in ensuring security are access to shared and sensitive medical data by malicious individuals and organ trafficking. These are followed by ensuring a fair and transparent approach to waiting lists and organ matching.

As can be seen from Table 4, the majority of research that describes their platforms suggests adopting Ethereum (11 out of 17) [19,57–59,61,64,66,67,70,75,76]. In the remaining six studies, three adopted Hyperledger Fabric [56,65,72], one used Monero [69], and two did not specify the platform they used [68,71].

Table 4. In-house-validated blockchain solutions are offered by the papers.

No.	Ref.	Purpose	BLOCKCHAIN									
			General Structure Features			**Smart Contract Features**		**Storage Features**			**Validation Features**	
			Blockchain Platform	**Chain Type**	**Consensus**	**Smart Contracts**	**Prg. Lang.**	**Platform**	**On-Chain Data Type**	**Off-Chain Data Type**	**Platform**	**Metric(s)**
1	[19]	Matching incompatible alive kidney donor pairs with compatible recipients	Ethereum	Public	PoC, PoM	√	Solidity	×	CertificateID, RecipientID, RecipientHealth, DonorID, DonorHealth, address DoctorSig, Contact, TimeStamp, ValidPair	Medical records, the hash of the donor and recipient pair	×	×
2	[56]	To enhance the transparency, immutability, confidentiality, and security	Hyperledger	Private	×	√	×	MongoDB, CouchDB	×	×	Chai and Mocha test	×
3	[57]	To automate the existing system	Ethereum	Public	PoW	√	Solidity	MongoDB, IPFS	As implied; transactional data	As implied; non-transactional data	Ganache	Gas cost, data size, and key size
4	[58]	To improve ownership for shared medical records	Ethereum	Private	PoA	√	Solidity	MongoDB, IPFS	Transactional data; does not include sensitive data	Non-transactional sensitive data	×	Gas cost, and data size
5	[59]	To remove trusted third party dependency	Ethereum	Private	×	√	Solidity	EVM	Transactional data; does not include sensitive data	×	Ganache and smoke testing	Gas cost
6	[61]	To provide reliable and accurate data for Smart ID (Ethereum Smart Contract address)	Ethereum	×	×	√	Solidity	MySQL, XAMPP	Hash representations of identity data	×	Visual Studio Code, IntelliJ, and Sublime text	×
7	[64]	To provide a reliable platform	Ethereum	×	×	√	Solidity	×	×	×	TestRPC (Ganache)	×
8	[65]	To ensure the security of the shared medical data	Hyperledger	Private	×	√	×	×	Transactional data; does not include sensitive data	Non-transactional sensitive data	×	×
9	[66]	To track data for verification	Ethereum	×	×	√	×	MySQL	All transplant, organ list, and waiting list information	The changing values	Ganache	Response time, deployment gas cost

Table 4. *Cont.*

			BLOCKCHAIN									
			General Structure Features			Smart Contract Features			Storage Features		Validation Features	
No.	**Ref.**	**Purpose**	**Blockchain Platform**	**Chain Type**	**Consensus**	**Smart Contracts**	**Prg. Lang.**	**Platform**	**On-Chain Data Type**	**Off-Chain Data Type**	**Platform**	**Metric(s)**
10	[67]	To enhance secure, traceable, auditable, private, and trustworthy	Ethereum	Private	×	√	Solidity	EVM	Details of waiting list, donors, and matching results	×	Oyente	×
11	[68]	To track of the donation	×	×	×	×	×	Local DB	×	×	×	×
12	[69]	For secure and anonymous patient identification	Monero	×	×	×	×	Private IPFS	Ref. (data pointer) to the encrypted biometric template	Personal sensitive data	×	Computational cost
13	[70]	To provide a secure and transparent system	Ethereum	×	×	√	×	MongoDB, IPFS	Transactional data	Personal information and medical records	Goerli	×
14	[71]	Secure and translucent system to sensitive data access	×	×	×	√	×	IPFS	Transactional data; does not include sensitive data	Non-transactional sensitive data	×	Execution time, data size, throughput
15	[72]	To build up a secure and transparent system	Hyperledger	Private	RAFT	√	×	CouchDB	×	×	Amazon Web Services (AWS)	Throughput, latency, successful/failed transactions count, resources
16	[75]	To facilitate the secure and transparent sharing of data	Ethereum	Private	×	√	Solidity	×	Medical data, including medical history, blood type, organ status, matching information	×	×	×
17	[76]	To ensure security	Ethereum	Private	×	√	×	×	×	×	×	×

A recently published study [69] suggested a biometric authentication protocol that permits data processing and storage in an encrypted manner when integrated into a blockchain that is based on a cryptocurrency that prioritises privacy. The research suggests using the public blockchain to handle the infrastructure needed for online verification, thereby offering an encrypted area for offline processing and storage. On the other hand, it was not surprising, given the characteristics of the proposed platforms, that further research was utilising Ethereum's smart contract features.

As can be seen in Table 4, eight out of ten research studies that discuss blockchain encourage utilising private blockchain [56,58,59,65,67,72,75,76], whilst the other two studies suggest using public blockchain [19,58]. Users have a definite advantage when using a private blockchain because of its improved security, easier authentication, and scalability. This makes it the recommended blockchain type to utilise for the OTP, where numerous stakeholders share sensitive information that needs to be kept private and secure. It is important to note that, despite the fact that private blockchain is better and more suitable for the use-case of the OTP participants with similar characteristics at the same level, no research has investigated or recommended a hybrid or consortium blockchain-based approach that would be more suitable for the intricate OTP structure.

It was unexpected that most of the papers did not provide details about the consensus mechanisms used. Consensus protocol details were provided for only four investigations. These include RAFT [72], proof of work [57], proof of authority [58], and proof of concept/proof of match [19]. It is thought that the fact that the OTP requirements involve sharing sensitive data with several stakeholders is the reason why alternate consensus methods, aside from proof of work, exist in this research. However, because consensus mechanisms are used to ensure the blockchain features, like reliability, consistency, and attack resistance, and have a complex infrastructure, and some consensus algorithms consume a lot of energy, researchers may not have disclosed the details on this issue in order to avoid criticism. Thus, this may provide an explanation for the 13 investigations where no information was supplied regarding consensus processes.

Apart from [68,69], the remaining papers provide details regarding the smart contracts used. These details encompass various categories such as algorithm architecture, pseudo code, smart contracts, and the subjects guiding the system architecture's development. Most of the studies delve into the specifics of pseudo code and smart contract algorithms. Notably, eight of them do not disclose the programming language employed in the development of smart contracts.

For security and scalability, it is essential to decide in advance which data will be retained and where and how it will be retained. Terms related to data storage in the blockchain include "off-chain" and "on-chain." On-chain data, usually distributed as a copy held by all participants of the entire blockchain network, consists of basic blockchain data (block header, transaction history, smart contract codes, etc.) and transactional data (executed transactions, smart contract interactions, transaction details, etc.). On the other hand, off-chain data refers to sensitive data such as personal medical records, medical images, or media content kept on a central server, a private cloud storage system, or a private network. One of the important criteria for scalability is data size. Developers need to carefully consider the issue of on-chain data storage. The first reason is data storage limitation; the second reason is that the cost increases as the data size increases, and the last one is that on-chain data must consist of compact data that are free of sensitive data in case of data leakage. The majority of the studies included in the evaluation (12 out of 17) provide information about the data storage platform (except [56,64,68,72,76]) (Table 4). Notably, five of them suggest that IPFS [57,58,69–71] should be used as the off-chain application strategy. The majority of studies (6 out of 17) advise keeping "transactional data; does not include sensitive data" as the on-chain data content option. They advise storing "any non-transactional sensitive data" on the IPFS platform as an off-chain data content solution (4 out of 8). Among the reasons why personal and sensitive shared health data are not kept on-chain are the ability to track data on the blockchain, the need to comply with regulations, increasing the database size, increasing the transaction cost, and difficulties in updating and making changes to data. Additionally, this could negatively impact the overall performance of the blockchain network. More than half of the studies we examined (9 out of 17) provide information about the test platform used for validation. Notably, four of them utilised the Ganache test platform, creating a local Ethereum network to test and develop smart contracts. However, only three of these studies [57,59,66] provided details on the metrics they analysed. It is worth mentioning that only one study employed the Oyente test platform [67], focusing on potential security issues by examining smart contract code, yet no information was shared regarding the test metrics. Additionally, despite one study mentioning the use of the Goerli test platform [70], which simulates a real Ethereum test network environment, it did not disclose the analysed metrics. Among the studies that shared details about test metrics [58–60,67,70,72,73], the majority predominantly used the "gas cost" metric, reflecting the natural choice due to the prevalence of the Ethereum platform in the analysed articles. The noteworthy point is that they do not provide all the details about the validation results. Conversely, it is important to highlight those four articles [57,59,66,72] provide comprehensive details regarding the validation features.

4.2.3. Fully Validated Blockchain Solution

This category investigates the developed solutions by considering how standardised and regulated the solution is and whether it is fully tested and deployed in a real work environment using real data. It is important to note that, upon evaluation of all the solutions in the papers examined, none of them fell into the "fully verified Blockchain solution" category. This observation is attributed to the early stages of maturity in the respective studies. Additionally, the choice of test settings depends on factors such as the desired blockchain platform, type of chain, and consensus process. The parameters considered vary based on the testing platform employed. The existence of different verification environments and metrics in various studies implies that the standardisation effort is still in its initial phases, and there is currently no established framework for verifying such systems.

5. Issues and Challenges

5.1. Blockchain Technologies Dedicated to OTP

Many OTP applications based on blockchain designate doctors, donors, and recipients as end users. In private chain setups recommended for OTP use, doctors are identified as verification nodes. Typically, doctors wield complete authority in overseeing medical procedures within the OTP, confirming donors and recipients in the system. Conversely, system administrators are often designated as verification nodes, akin to traditional database administration, facilitating routine transactions involving the identification of healthcare providers, hospitals, and other stakeholders in the system. This scenario appears inseparable from the evolution of private chain preferences and application instances in the realm of conventional database management. Another perspective is that the intricacies of the OTP constitute the primary driver behind this standpoint.

A chronological assessment of studies reveals a shift in the strategy of on-chain data storage. Initially, systems were designed to store all data on-chain. This approach has transformed over time, moving from on-chain storage of data pointers and pseudoIDs for sensitive information in physical databases or IPFS to the current trend of storing data directly on-chain. Additionally, there is a noteworthy transition from endorsing blockchain implementations as the proposed solution to the integration of other technologies into blockchain-based applications.

Additionally, BlockAsp can be used for blockchain model-checking, including smart contracts. With this method, security elements can be easily incorporated into the contract logic [77]. Additionally, "the advanced observe-based statistical model-checking (OSM) framework", which uses "aspect-oriented programming", can be used to increase the reliability and adaptability of systems where sensitive medical data is kept in dynamic environments such as the OTP [78].

5.2. Privacy and Anonymity

In certain studies, it is challenging to assert that user anonymity, particularly for donors and recipients, is adequately ensured. The complexities arise from organ-matching, waiting-list management, and priority scenarios for donors and recipients, presenting significant hurdles. A noteworthy evolution since the initial studies is the shift towards adopting the perspective of retaining zero personal data on the chain. While this development is positive, there is a requirement for integrations and emerging trends that further enhance anonymity. It becomes imperative to identify blockchain frameworks, consensus algorithms, and integrable technologies deemed suitable for the OTP, considering the evolving landscape.

5.3. Performance and Scalability

Applications that are created especially for the OTP have to grow easily. Orientation towards the use of blockchain is crucial for this. Although using blockchain for the OTP increases trust, efforts should be taken to make sure that performance and scalability are optimised to the highest degree possible. Introducing innovative technology like blockchain would undoubtedly help with these endeavours.

5.4. Standardisation

Although our survey revealed that Ethereum and private chains are more proposed among blockchain platforms and chain types, there are also examples where other platforms and chain types are used. The challenge is that it becomes clear that there is no agreement on which blockchain type or platform is most suitable for which scenario of the OTP steps. However, another challenge is that researchers have not yet reached an agreement on which consensus mechanism to use for which use-case. It is observed that each researcher who makes proposals about consensus uses a different technique. Additionally, it is worth noting that the design objectives of the smart contracts devised for the OTP are dispersed across a broad spectrum. This is believed to stem from the absence of a standardised approach regarding which processes should be automated for the OTP. On the other hand, the choices in storage options, verification methods selected, and the prevalence of usage also indicate the lack of a standardised approach in the OTP. While the blockchain field has a trend in which studies on standardisation are rapidly progressing, the OTP seems to be at the beginning of the development phase in this regard. These pathways should also be followed by OTP developers in order to find, standardise, and incorporate the blockchain technologies that best fit their industry.

5.5. Testing and Verification Environments

The OTP holds critical significance, particularly concerning issues related to organ trafficking and unauthorised access by malicious individuals. Hence, it is essential to thoroughly establish security and reliability measures. It was identified that among the articles included in the review, those with "in-house validated Blockchain solutions" did not adequately provide details about their validation process. Additionally, it is worth noting the absence of articles with a "full-validated Blockchain solution." Consequently, any application or improvement developed for the OTP should undergo comprehensive testing and verification to ensure its effective performance not only in controlled laboratory settings but also in real-world scenarios. The key elements in this regard emphasise the necessity of developing standardised testing environments that facilitate comparisons and enable the thorough assessment of functionalities.

5.6. Regulation

The fact that blockchain technology is not recognised by the present legal regulations or is subject to restrictions is a significant obstacle. The adoption and deployment of blockchain in the OTP are hampered by the lack of a legal framework. As a result, fresh legislation is required to facilitate the application of blockchain technology. It is possible to create regulations that guarantee the data generated by blockchain-based systems can be utilised as trustworthy and irrefutable evidence against medical facilities, insurance providers, and legal authorities.

5.7. Interoperability

The analysis of blockchain-based OTP solution proposals within the scope of the review has revealed instances where different platforms are preferred. Consequently, the utilisation of multiple platforms poses significant challenges to interoperability, especially considering the international dimension of the OTP. This challenge stems from the fact that each blockchain network consists of various platforms with their own protocols, consensus mechanisms, and smart contract languages. Integrating different platforms presents difficulties in ensuring seamless interoperability. Potential challenges may arise from concerns such as data integrity and consistency, identity management (particularly concerning the verification of donors, recipients, and healthcare providers), individual consent and data ownership, existing on-chain and off-chain preferences, and smart contract software security. Furthermore, compliance with national and international regulations and standards further complicates the matter. While there exist inter-chain communication protocols and interoperability solutions enabling transactions and data transfer between different blockchain networks (such as atomic swaps, cross-chain communication, token bridges, etc.), these solutions are not yet mature for complex systems such as the OTP. Hence, specialised solutions are needed to be tailored to facilitate the realisation of national and international OTPs, addressing their unique requirements.

6. Conclusions and Future Work

The fundamental contributions of blockchain-based applications include preventing unnecessary data storage (data redundancy), ensuring the immutability of records to provide reliable and accurate data, eliminating the rigidity of centralised management through decentralisation, enabling parties to conduct transactions within a framework of mutual trust, and increasing traceability, accountability, and transparency due to having a form of chronological encrypted data record. In this paper, we conducted a systematic literature review encompassing all relevant studies examining the integration of blockchain into OTP solutions, describing the theoretical and technical perspectives they offer. Through our systematic review, we have observed a significant and increasing interest in this field, despite being relatively new, with a growing number of studies each year. Blockchain technology is predominantly utilised to enhance security, transparency, tracking, confidentiality, and trustworthiness. We categorised the blockchain-based solutions provided by the studies according to the maturity levels we assessed in terms of validation. We determined that the majority of studies are at the stage of “in-house validated Blockchain solutions” and elaborated on the technical aspects. Additionally, the absence of a study at the level of a “full-validated Blockchain solution” was both surprising and indicative of a gap in the literature. In this context, the need for research on the environments to be used in validation and the standards these environments should meet is highlighted. Moreover, this situation also underscores the need for research on the datasets to be used for validation. On the other hand, there is a need for further research dedicated to the OTP, including blockchain framework, consensus algorithms, smart contracts, and integration with conventional systems.

If we briefly delve into this topic, consensus algorithms emerge as one of the foremost challenges to address. The consensus algorithm to be utilised for the OTP, which involves sensitive and multi-stakeholder shared data, must address concerns regarding privacy and confidentiality. Priority should be given to the consensus algorithms that ensure transparency and auditability while safeguarding sensitive information. Additionally, the consensus algorithms should demonstrate the utmost resilience against various attacks such as Sybil attacks (attempting to control a network by creating multiple fake identities), double-spending attacks (spending the same electronic asset twice), and 51% attacks (where an individual or group seizes the majority of the network's hash power). Furthermore, many consensus algorithms like proof of work have been proven to require significant computational power and energy consumption. Therefore, there should be a consideration for employing energy-efficient consensus algorithms that minimise energy consumption without jeopardising the security and integrity of the blockchain [79].

Thorough on-site analysis of pertinent legal, medical, and technological factors is crucial for customising smart contract design. This approach facilitates overcoming the intricate nature of OTPs. Achieving an effective and robust solution necessitates collaboration among domain experts to ensure compliance with medical procedures and legal and ethical considerations. In this way, easy-to-use and adopted solutions can be developed. In the OTP, the customisation of smart contracts can be exemplified as follows: The customisation process of smart contract design should start by identifying stakeholders such as donors, recipients, transplant teams, and procurement organisations who will be involved in the contract. The roles and responsibilities of all stakeholders should be clearly defined individually. Specific terms and conditions are established among the parties to determine the contract terms. Attention is paid to designing these as smart contract pieces that are compatible with donor consent, organ-matching algorithms, waiting lists, organ allocation rules, medical criteria, and legal requirements and customised for each situation. One crucial aspect is to determine reliable data sources to feed smart contracts. The accuracy and reliability of identified data sources are critical to ensure the integrity of smart contracts. Integrated data sources may include electronic medical records, organ waiting lists, organ allocation and procurement databases, etc. Additionally, the programming logic governing the behaviour of smart contracts should be specifically developed for OTPs. In addition, the programming logic that governs the behaviour of the smart contract should be developed specifically for the OTP. This logic should, at a minimum, include validation of the data inputs, verification of compliance with predefined rules, and execution of the actions according to certain conditions. For instance, the smart contract can automatically verify donor and recipient compatibility, considering medical criteria. Moreover, there is a need to ensure that appropriate security measures are in place to safeguard the privacy, integrity, and availability of smart contracts and related data. Encryption, access controls, and audit trails can be utilised to prevent unauthorised access and tampering. It is possible to choose not to store sensitive medical data on-chain. If deemed necessary to perform such operations, distributed solutions such as IPFS can be used to store medical data. After smart contracts are deployed to the blockchain networks, there are varying levels of manageability constraints depending on the platform and type of blockchain used. Hence, it is crucial to thoroughly verify the accuracy and security of the smart contracts before they are placed on the blockchain. Once validated, smart contracts can be deployed to a suitable blockchain platform. [80].

In the context of the OTP, electronic medical records managed through traditional methods are maintained and processed within specific legal regulations and standards. Examples of these include the GDPR, the International Information Technology standard ISO/IEC 27001 [81], and Health Level Seven (HL7). Ensuring compliance of blockchain-based systems with these regulations would enhance their ability to integrate with existing systems. Key challenges in this regard include ensuring compliance with the GDPR, regulations that vary between countries, and the lack of OTP-specific standardisation. While efforts by countries to establish the legal framework for blockchain are observed, it is anticipated that efforts to make it legally admissible in the OTP domain will take time. Additionally, due to its inclusion of sensitive medical data and the complex nature of the system, it is also likely that this process will take longer than anticipated.

On the other hand, the absence of a "full validation" blockchain application specifically developed for the OTP is also a significant challenge. Among the limitations of test environments is the lack of a dedicated test environment for the OTP. Additionally, the ethical dimension of simulation on real-world datasets is another constraint. Furthermore, while centres like Eurotransplant in Europe and the Organ Procurement Organization (OPO) in America provide researchers with test data, the lack of public datasets suitable in quality and quantity for developing realistic test environments adds another layer of difficulty. Despite the potential of blockchain for digital transformation in the OTP, the issue of adoption by patients and healthcare professionals is currently being hindered by the aforementioned challenges. Uncertainties regarding the privacy, security, and conditions under which recorded data is processed and shared contribute to apprehension among end users [82].

In summary, developing new consensus algorithms, customising smart contract design for this field, enhancing validation environments to support "full validation", standardisation, and the need for required regulations require more research for the successful and widespread implementation of blockchain solutions dedicated to the OTP. The need for specialised developers focused on this field is also undeniable. In this context, the adoption of blockchain will be further facilitated.

Author Contributions: Conceptualisation, E.C. and M.B.; methodology, E.C. and M.B.; formal analysis, E.C. and M.B.; investigation, E.C. and M.B.; resources, M.B.; writing—original draft preparation, E.C. and M.B.; writing—review and editing, E.C. and M.B.; supervision, M.B.; project administration, M.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Karabük University under grant number KBÜBAP-22-UIP-163 and supported by Science Foundation Ireland under grant numbers 13/RC/2106/P_2 (ADAPT SFI Research Centre for AI-Driven Digital Content Technology) and 13/RC/2094/P_2 (Lero SFI Centre for Software). For the purpose of open access, the author has applied a CC BY public copyright licence to any author-accepted manuscript version arising from this submission.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. EDQM Publishes 8th Edition of the Guide to the Quality and Safety of Organs for Transplantation. Available online: https://www.edqm.eu/en/-/edqm-publishes-revised-and-updated-of-organ-transplantation-guide-8th-edition-1 (accessed on 3 January 2024).
2. Howell, A.; Saber, T.; Bendechache, M. Measuring node decentralisation in blockchain peer to peer networks. *Blockchain Res. Appl.* **2022**, *4*, 100109. [CrossRef]
3. Bendechache, M.; Saber, T.; Muntean, G.M.; Tal, I. Application of Blockchain technology to 5g-enabled vehicular networks: Survey and future directions. In Proceedings of the International Symposium on High Performance Mobile Computing & Wireless Networks for HPC (MCWN 2020), Barcelona, Spain, 10–14 December 2020.
4. Wenhua, Z.; Qamar, F.; Abdali, T.-A.N.; Hassan, R.; Jafri, S.T.A.; Nguyen, Q.N. Blockchain Technology: Security Issues, Healthcare Applications, Challenges and Future Trends. *Electronics* **2023**, *12*, 546. [CrossRef]
5. Khan, D.; Jung, L.T.; Hashmani, M.A. Systematic Literature Review of Challenges in Blockchain Scalability. *Appl. Sci.* **2021**, *11*, 9372. [CrossRef]
6. Girlanda, R. Deceased organ donation for transplantation: Challenges and opportunities. *World J. Transplant.* **2016**, *6*, 451–459. [CrossRef] [PubMed]
7. Beyar, R. Challenges in Organ Transplantation. *Rambam Maimonides Med. J.* **2011**, *2*, e0049. [CrossRef] [PubMed]
8. Miao, Y.; Gai, K.; Zhu, L.; Choo, K.-K.R.; Vaidya, J. Blockchain-based Shared Data Integrity Auditing and Deduplication. *IEEE Trans. Dependable Secur. Comput.* **2023**, 1–16, *Early Access*. [CrossRef]
9. Gai, K.; Wu, Y.; Zhu, L.; Qiu, M.; Shen, M. Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3548–3558. [CrossRef]
10. Haque, A.B.; Islam, A.K.M.N.; Hyrynsalmi, S.; Naqvi, B.; Smolander, K. GDPR Compliant Blockchains–A Systematic Literature Review. *IEEE Access* **2021**, *9*, 50593–50606. [CrossRef]
11. Zou, W.; Lo, D.; Kochhar, P.S.; Le, X.-B.D.; Xia, X.; Feng, Y.; Chen, Z.; Xu, B. Smart Contract Development: Challenges and Opportunities. *IEEE Trans. Softw. Eng.* **2021**, *47*, 2084–2106. [CrossRef]
12. Gai, K.; Zhang, Y.; Qiu, M.; Thuraisingham, B. Blockchain-Enabled Service Optimizations in Supply Chain Digital Twin. *IEEE Trans. Serv. Comput.* **2022**, *16*, 1673–1685. [CrossRef]
13. Gai, K.; Guo, J.; Zhu, L.; Yu, S. Blockchain Meets Cloud Computing: A Survey. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 2009–2030. [CrossRef]
14. Balasubramanian, S.; Shukla, V.; Sethi, J.S.; Islam, N.; Saloum, R. A readiness assessment framework for Blockchain adoption: A healthcare case study. *Technol. Forecast. Soc. Change* **2021**, *165*, 120536. [CrossRef]

15. Anselmo, A.; Materazzo, M.; Di Lorenzo, N.; Sensi, B.; Riccetti, C.; Lonardo, M.T.; Pellicciaro, M.; D'amico, F.; Siragusa, L.; Tisone, G. Implementation of Blockchain Technology Could Increase Equity and Transparency in Organ Transplantation: A Narrative Review of an Emergent Tool. *Transpl. Int.* **2023**, *36*, 10800. [CrossRef] [PubMed]
16. Niyigena, C.; Seol, S.; Lenskiy, A. Survey on Organ Allocation Algorithms and Blockchain-based Systems for Organ Donation and Transplantation. In Proceedings of the 2020 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 21–23 October 2020; pp. 173–178.
17. George, L.; Kizhakkethottam, J.J. A Survey on the Impact of Blockchain in Effective Organ Transplantation. In Proceedings of the 2023 IEEE International Conference on Recent Advances in Systems Science and Engineering (RASSE), Kerala, India, 8–11 November 2023; pp. 1–6.
18. Soltanisehat, L.; Alizadeh, R.; Hao, H.; Choo, K.-K.R. Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review. *IEEE Trans. Eng. Manag.* **2023**, *70*, 353–368. [CrossRef]
19. Zouarhi, S. Kidner—A Worldwide Decentralized Matching System for Kidney Transplants. *J. Int. Soc. Telemed. Ehealth* **2017**, *5*, 1–4. Available online: https://journals.ukzn.ac.za/index.php/JISfTeH/article/view/287 (accessed on 7 January 2024).
20. Gaynor, M.; Tuttle-Newhall, J.; Parker, J.; Patel, A.; Tang, C. Adoption of Blockchain in Health Care. *J. Med. Internet Res.* **2020**, *22*, e17423. [CrossRef] [PubMed]
21. Carrano, F.M.; Sileri, P.; Batt, S.; Di Lorenzo, N. Blockchain in surgery: Are we ready for the digital revolution? *Updates Surg.* **2022**, *74*, 3–6. [CrossRef]
22. Varshney, S.; Kansra, P.; Garg, A. Policy Suggestions for Transplantation of Organs in India: Use of Blockchain Technology to Manage Organ Donation. *Indian J. Transplant.* **2023**, *17*, 339–342. [CrossRef]
23. Chavez, N.; Kendzierskyj, S.; Jahankhani, H.; Hosseinian, A. Chapter—Securing transparency and governance of organ supply chain through Blockchain. In *Policing in the Era of AI and Smart Societies*; Jahankhani, H., Akhgar, B., Cochrane, P., Dastbaz, M., Eds.; Springer Nature: Cham, Switzerland, 2020; pp. 97–118.
24. Morande, S.; Marzullo, M. Application of Artificial Intelligence and Blockchain in Healthcare Management–Donor Organ Trans-plant System. *Ann. Manag. Organ. Res.* **2020**, *1*, 25–38.
25. Shuhaiber, A.; Nizamuddin, N.; Amer, A. Breaking Boundaries: Exploring Blockchain's Impact on UAE Organizations. In Proceedings of the 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA), Kuwait City, Kuwait, 24–26 October 2023; pp. 12–21.
26. Alam, T.; Raza, K. Chapter 7—Blockchain technology in healthcare: Making digital healthcare reliable, more accurate, and revolutionary. In *Advances in Ubiquitous Sensing Applications for Healthcare, Translational Bioinformatics in Healthcare and Medicine*; Raza, K., Dey, N., Eds.; Academic Press: Cambridge, MA, USA, 2021; Volume 13, pp. 81–96. [CrossRef]
27. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*; SSRN, 2008; pp. 1–9. Available online: https://ssrn.com/abstract=3440802 (accessed on 24 April 2024).
28. Merkle, R.C. Protocols for Public Key Cryptosystems. In Proceedings of the 1980 IEEE Symposium on Security and Privacy, Oakland, CA, USA, 14–16 April 1980.
29. Szabo, N. Smart contracts: Building blocks for digital markets. *EXTROPY J. Transhumanist Thought* **1996**, *16*, 1–11. Available online: https://www.truevaluemetrics.org/DBpdfs/BlockChain/Nick-Szabo-Smart-Contracts-Building-Blocks-for-Digital-Markets-1996-14591.pdf (accessed on 24 April 2024).
30. Narayanan, A.; Clark, J. Bitcoin's academic pedigree. *Commun. ACM* **2017**, *60*, 36–45. [CrossRef]
31. Merkle, R.C. A Certified Digital Signature. In Proceedings of the Conference on the Advances in Cryptology—CRYPTO'89, 9th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 1989; pp. 218–238. [CrossRef]
32. Monrat, A.A.; Schelen, O.; Andersson, K. A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities. *IEEE Access* **2019**, *7*, 117134–117151. [CrossRef]
33. Chaum, D. *Blind Signatures for Untraceable Payments*; Springer: Berlin/Heidelberg, Germany, 1982.
34. Haber, S.; Stornetta, W.S. *How to Time-Stamp a Digital Document, Advances in Cryptology-CRYP'O'90*; Menezes, A.J., Vanstone, S.A., Eds.; Springer: Berlin/Heidelberg, Germany, 1991; Volume 537, pp. 437–455.
35. Bayer, D.; Haber, S.; Stornetta, W.S. Improving the Efficiency and Reliability of Digital Time-Stamping. In *Methods in Communication, Security, and Computer Science*; Capocelli, R., De Santis, A., Vaccaro, U., Eds.; Springer: New York, NY, USA, 1992; pp. 329–334.
36. Back, A. Hashcas—A Denial of Service Counter-Measure, 1 August 2002. Available online: http://www.hashcash.org/papers/hashcash.pdf (accessed on 3 January 2024).
37. Back, A. Hash Cash Postage Implementation, 28 March 1997. Available online: http://www.hashcash.org/papers/announce.txt (accessed on 23 April 2013).
38. Szabo, N. Bit-Gold, 1998. Available online: https://www.difotech.it/immagini_articolo/Nick-Szabo/Unenumerated_Bit_gold_inglese.pdf (accessed on 2 March 2023).
39. Dai, W. B-Money, 1998. Available online: http://www.weidai.com/bmoney.txt (accessed on 3 March 2023).
40. Saroiu, S.; Gummadi, P.K.; Gribble, S.D. Measurement study of peer-to-peer file sharing systems. In Proceedings of the Multimedia Computing and Networking, San Jose, CA, USA, 23–24 January 2002; Kienzle, M.G., Shenoy, P.J., Eds.; SPIE Digital Library: San Jose, CA, USA, 2001; Volume 4673, pp. 156–170. [CrossRef]

41. Finney, H. Rpow-Reusable Proofs of Work, 2004. Available online: http://web.archive.org/web/20071222072154/http://rpow.net/ (accessed on 1 March 2023).
42. Sunyaev, A. Distributed ledger technology. In *Internet Computing*; Springer: Berlin/Heidelberg, Germany, 2020; pp. 265–299. [CrossRef]
43. Zheng, G.; Gao, L.; Huang, L.; Guan, J. Decentralized Application (DAp"). In *Ethereum Smart Contract Development in Solidity*; Springer: Singapore, 2021; pp. 253–280. [CrossRef]
44. Buterin, V. Ethereum: A Next-Generation Smart Contract and Decentralized Application. 2014. Available online: https://finpedia.vn/wp-content/uploads/2022/02/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (accessed on 3 January 2024).
45. Altaleb, H.; Zoltan, R. Decentralized autonomous organizations review, importance, and applications. In Proceedings of the 2022 IEEE 26th International Conference on Intelligent Engineering Systems (INES), Crete, Greece, 12–15 August 2022; pp. 000121–000126.
46. Bhutta, M.N.M.; Khwaja, A.A.; Nadeem, A.; Ahmad, H.F.; Khan, M.K.; Hanif, M.A.; Song, H.; Alshamari, M.; Cao, Y. A Survey on Blockchain Technology: Evolution, Architecture and Security. *IEEE Access* **2021**, *9*, 61048–61073. [CrossRef]
47. Xie, J.; Tang, H.; Huang, T.; Yu, F.R.; Xie, R.; Liu, J.; Liu, Y. A Survey of Blockchain Technology Applied to Smart Cities: Research Issues and Challenges. *IEEE Commun. Surv. Tutorials* **2019**, *21*, 2794–2830. [CrossRef]
48. Tasdelen, A. *Chapter-2; Fundamentals of Blockchain. Exploring Blockchain Applications*, 1st ed.; Bozkus Kahyaoglu, S., Tecim, V., Eds.; CRC Press: Boca Raton, FL, USA, 2024; pp. 6–25. [CrossRef]
49. Kitchenham, B. *Procedures for Performing Systematic Reviews*; Keele University: Newcastle, UK, 2004; Volume 33, pp. 1–26.
50. Kitchenham, B.; Pretorius, R.; Budgen, D.; Brereton, O.P.; Turner, M.; Niazi, M.; Linkman, S. Systematic literature reviews in software engineering—A tertiary study. *Inf. Softw. Technol.* **2010**, *52*, 792–805. [CrossRef]
51. Kitchenham, B.; Brereton, P. A systematic review of systematic review process research in software engineering. *Inf. Softw. Technol.* **2013**, *55*, 2049–2075. [CrossRef]
52. Wohlin, C.; Prikladniki, R. Systematic literature reviews in software engineering. *Inf. Softw. Technol.* **2013**, *55*, 919–920. [CrossRef]
53. Feyer, S.; Siebert, S.; Gipp, B.; Aizawa, A.; Beel, J. Integration of the Scientific Recommender System Mr. DLib into the Reference Manager JabRef. In Proceedings of the European Conference on Information Retrieval, Aberdeen, UK, 8–13 April 2017; pp. 770–774.
54. Alandjani, G. Blockchain based auditable medical transaction scheme for organ transplant services. In Proceedings of the 5th International Conference on Green Computing and Engineering Technologies, Casablanca, Morocco, 17–19 September 2019; pp. 41–63. [CrossRef]
55. Dajim, L.A.; Al-Farras, S.A.; Al-Shahrani, B.S.; Al-Zuraib, A.A.; Merlin Mathew, R. Organ Donation Decentralized Application Using Blockchain Technology. In Proceedings of the 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 1–3 May 2019; pp. 1–4.
56. Lamba, R.; Gupta, Y.; Kalra, S.; Sharma, M. Preventing Waiting List Manipulation and Black Marketing of Donated Organs Through Hyperledger Fabric. In Proceedings of the 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 18–19 October 2019; pp. 280–285.
57. Ranjan, P.; Srivastava, S.; Gupta, V.; Tapaswi, S.; Kumar, N. Decentralised and Distributed System for Organ/Tissue Donation and Transplantation. In Proceedings of the 2019 IEEE Conference on Information and Communication Technology (CICT), Allahabad, India, 6–8 December 2019; pp. 1–6.
58. Daniel, I.A.; Pop, C.; Anghel, I.; Antal, M.; Cioara, T. A Blockchain based solution for Managing Transplant Waiting Lists and Medical Records. In Proceedings of the 2020 IEEE 16th International Conference on Intelligent Computer Communication and Processing (ICCP), Cluj-Napoca, Romania, 3–5 September 2020; pp. 505–510.
59. Kulshrestha, A.; Mitra, A.; Amisha. Securing Organ Donation using Blockchain. *Int. J. Sci. Eng. Res.* **2020**, *11*, 147–151.
60. Pillai, B.G.; Madhurya, J.A.; Jecob, J. An effective protection of data for organ donation using blockchain technology. *Int. J. Electr. Eng. Technol.* **2020**, *11*, 73–82. [CrossRef]
61. Wijayathilaka, P.L.; Gamage, P.P.; De Silva, K.H.B.; Athukorala, A.P.P.S.; Kahandawaarachchi, K.A.D.C.P.; Pulasinghe, K.N. Secured, Intelligent Blood and Organ Donation Management System—"LifeShare". In Proceedings of the 2020 2nd International Conference on Advancements in Computing (ICAC), Malabe, Sri Lanka, 10–11 December 2020; pp. 374–379.
62. Yahaya, C.A.C.; Firdaus, A.; Khen, Y.Y.; Yaakub, C.Y.; Razak, M.F.A. An Organ Donation Management System (ODMS) based on Blockchain Technology for Tracking and Security Purposes. In Proceedings of the 2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM), Pekan, Malaysia, 24–26 August 2021; pp. 377–382.
63. Soni, A.; Ganesh Kumar, S. Creating Organ Donation System with Blockchain Technology. *Eur. J. Mol. Clin. Med.* **2021**, *8*, 2387–2395.
64. Begum, A.; Ayushi Dixit, A.; Mukherjee, A. OraB—A Community of Donors. In Proceedings of the 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 15–16 July 2022; pp. 1–6.
65. Çalık, E.; Kaya, H.; Çelebi, F.V. A novel method to ensure the security of the shared medical data using smart contracts: Organ transplantation sample. *Concurr. Comput. Pract. Exp.* **2022**, *34*, e6752. [CrossRef]

66. Chaudhary, N.; Manvi, S.S.; Koul, N. Organ Bank Based on Blockchain. In Proceedings of the 2022 IEEE International Conference on Electronics, Computing and Communication Technologies (CONECCT), Bangalore, India, 8–10 July 2022; pp. 1–5.
67. Hawashin, D.; Jayaraman, R.; Salah, K.; Yaqoob, I.; Simsekler, M.C.E.; Ellahham, S. Blockchain-Based Management for Organ Donation and Transplantation. *IEEE Access* **2022**, *10*, 59013–59025. [CrossRef]
68. Yashwanth Kumar, G.N.; Supreetha, M. Smart NGO Tracking System Using Blockchain Technology. In Proceedings of the 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), Mysuru, India, 16–17 October 2022; pp. 1–6.
69. Sarier, N.D. Privacy Preserving Biometric Authentication on the blockchain for smart healthcare. *Pervasive Mob. Comput.* **2022**, *86*, 101683. [CrossRef]
70. Ajay, G.; Lokesh, A.; Sravanasandhya, D.; Kousalya, G.; Teja, D.D.; Daniya, T. A Web DApp for Efficient Organ Donation Man-agement System: Leveraging Centralized Wallet Architecture as Backend. In Proceedings of the 2023 2nd International Conference on Applied Artificial Intelligence and Computing (ICAAIC), Salem, India, 4–6 May 2023; pp. 666–672.
71. Divyashree, D.; Ravi, C. Blockchain-Based Access-Control System for Unused Medicine and Organ Donation Using Enhanced Hybrid Cryptography. In Proceedings of the 2023 International Conference on Network, Multimedia and Information Technology (NMITCON), Bengaluru, India, 1–2 September 2023; pp. 1–8.
72. Ghosh, S.; Dutta, M. Indriya: Building a Secure and Transparent Organ Donation System with Hyperledger Fabric. *TechRxiv* **2023**. [CrossRef]
73. Shymala, B.; Solana, M.; Saranya, P.; Swetha, M. Organ Donation and Transplantation Framework based on Ethereum Blockchain. In Proceedings of the International Conference on Innovative Computing & Communication (ICICC), Delhi, India, 19–20 February 2022. [CrossRef]
74. Hovorushchenko, T.; Hnatchuk, Y.; Osyadlyi, V.; Kapustian, M.; Boyarchuk, A. Blockchain-Based Medical Decision Support System. *J. Cyber Secur. Mobil.* **2023**, *12*, 253–274. [CrossRef]
75. Kayalvili, S.; Saranya, S.; Pushparaj, E.; Sanjay, S. Management of Organ Donation Using Dapp in Blockchain. *Int. J. New Innov. Eng. Technol.* **2023**, *22*, 74–80.
76. Thaker, R.; Saxena, K.; Adappa, V.; Raghuvanshi, R. ORGANiser. In Proceedings of the 2023 International Conference on Advanced Computing Technologies and Applications (ICACTA), Mumbai, India, 6–7 October 2023; pp. 1–5.
77. AlSobeh, A.M.R.; Magableh, A.A. BlockASP: A Framework for AOP-Based Model Checking Blockchain System. *IEEE Access* **2023**, *11*, 115062–115075. [CrossRef]
78. AlSobeh, A.M.R. OSM: Leveraging model checking for observing dynamic behaviors in aspect-oriented applications. *Online J. Commun. Media Technol.* **2023**, *13*, e202355. [CrossRef]
79. Hussein, Z.; Salama, M.A.; El-Rahman, S.A. Evolution of blockchain consensus algorithms: A review on the latest milestones of blockchain consensus algorithms. *Cybersecurity* **2023**, *6*, 30. [CrossRef]
80. Kannengiesser, N.; Lins, S.; Sander, C.; Winter, K.; Frey, H.; Sunyaev, A. Challenges and Common Solutions in Smart Contract Development. *IEEE Trans. Softw. Eng.* **2022**, *48*, 4291–4318. [CrossRef]
81. ISO/IEC 27001:2022(en). Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements. The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), 2022. Available online: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en (accessed on 24 April 2024).
82. Singh, D.; Monga, S.; Tanwar, S.; Hong, W.-C.; Sharma, R.; He, Y.-L. Adoption of Blockchain Technology in Healthcare: Challenges, Solutions, and Comparisons. *Appl. Sci.* **2023**, *13*, 2380. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.